## CLAIMS

What is claimed is:

1. An apparatus comprising:

an oscillator with an output signal dependant upon a random source;

a sampling device to sample the output signal from the oscillator to obtain a sampled oscillator output; and

a fixed frequency clock driven linear feedback shift register (LFSR) communicatively coupled to the sampling device via a digital gate to receive the sampled oscillator output, and to provide a random number at an output of the LFSR.

2. An apparatus as in claim 1, further comprising:

a processor communicatively coupled to the LFSR to read the random number, and to insert the random number into an algorithm to obtain a robust random number.

3. An apparatus as in claim 1, wherein the oscillator comprises at least two inverters.

4. An apparatus as in claim 1, wherein the sampling device comprises a flip-flop.

5. An apparatus as in claim 1 wherein the digital gate coupling the LSFR to the sampling devise comprises an exclusive-OR gate.

6. An apparatus as in claim 2, wherein the algorithm is a SHA-1 algorithm.

7. An apparatus as in claim 2, further comprising the processor to duplicate the random number at least once, the processor to concatenate the duplicated random numbers prior to inserting the concatenated duplicated random number into the algorithm, wherein subsequent robust random number calculations do not require initialization of any variables.

8. An apparatus as in claim 1, wherein the random source comprises at least one of shot noise, and switching noise from electrical components within the apparatus.

9. An apparatus as in claim 1, wherein the fixed frequency clock driven LFSR is coupled to the sampling device and to the output of the LFSR via the digital gate.

10. An apparatus as in claim 1, wherein the apparatus is implemented on an integrated circuit chip.

11. A method comprising:

generating random binary bits;

sampling and latching the generated random binary bits; and

inserting the generated random binary bits into a fixed frequency clock driven linear feedback shift register (LFSR) via a digital gate to generate a random number.

12. A method as in claim 11, further comprising

duplicating the generated random number at least once;

concatenating the duplicated random numbers; and inserting the generated random number into an algorithm to obtain a robust random number.

13. A method as in claim 12, wherein the algorithm is a SHA-1 algorithm.

14. A method as in claim 13 wherein the SHA-1 algorithm is initialized the first time the robust random number is generated.

15. An apparatus comprising:

a plurality of random oscillators each generating a random binary output signal, that includes at least a first oscillator and a second oscillator;

a plurality of sampling devices including at least a first sampling device and a second sampling device, wherein the first sampling device samples the output from the first oscillator and the second sampling device samples the output from the second oscillator; and

a fixed frequency clock driven linear feedback shift register (LFSR) that receives the sampled binary output signal from the first sampling device and the second sampled device to generate a random number.

16. An apparatus as in claim 15 further comprising a processor communicatively coupled to the LFSR to read the random number and to insert the random number in an algorithm to obtain a robust random number.

17. An apparatus as in claim 15 wherein each oscillator in the plurality of oscillators comprises at least two inverters.

18. An apparatus as in claim 15, wherein each sampling device in the plurality of sampling devices comprises a flip-flop.

19. An apparatus as in claim 15, wherein the LFSR receives the sampled binary output signal from the first sampling device and the second sampled device via a first exclusive OR gate and a second exclusive OR gate.

20. An apparatus as in claim 16, wherein the algorithm is a SHA-1 algorithm.

21. An apparatus as in claim 16, further comprising the processor to duplicate the random number at least once, the processor to concatenate the duplicated random numbers prior to inserting the concatenated duplicated random numbers into the algorithm.

22. An apparatus as in claim 15 wherein each random oscillator responds to at least one of shot noise and switching noise to generate a random frequency binary output signal.

23. A method for generating a robust random number using a mixing function comprising:
reading a seed from an entropy generator;
modifying the seed;
inserting the modified seed into the mixing function;
initializing a set of input variable used in the mixing function;
generating a robust random number using the mixing function; and

generating subsequent robust random numbers using the mixing function without re-initializing any of the set of input variables.

24. A method as in claim 23, wherein modifying the seed comprises:
duplicating a portion of the seed at least once;
concatenating the duplicated portions; and
padding the concatenated duplicated portions with a binary string to obtain a 512-bit modified seed

25. A method as in claim 23, wherein the mixing function is the SHA-1 algorithm.

26. A method as in claim 23, wherein the seed comprises 128 bits.

27. An apparatus comprising:
a processor to read a seed from an entropy generator, to modify the seed, to insert the modified seed into a mixing function, to initialize a set of input variables used in the mixing function to generate a robust random number, and to generate subsequent robust random numbers using the mixing function without re-initializing any of the set of input variables.

28. A apparatus as in claim 27, wherein the modified seed comprises:
the processor to duplicate a portion of the seed at least once;
the processor to concatenate the duplicated portions; and
the processor to pad the concatenated duplicated portions with a binary string to obtain a 512-bit modified seed.

29. The apparatus as in claim 27 wherein the mixing function is the SHA-1 algorithm.

30. The apparatus as in claim 27, wherein the seed comprises 128 bits.